

## REMARKS/ARGUMENTS

Claims 1-19 and 25-43 are pending in the application. Claims 1-19 are rejected as directed to non-statutory subject matter under 35 U.S.C. 101; claims 1-19 and 25-43 are rejected as containing subject matter which is not described in the specification under 35 U.S.C. 112, first paragraph; and Claims 1-19 and 25-43 are also rejected as anticipated under 35 U.S.C. 102(e). The rejection is traversed and reconsideration is requested. The references asserted do not teach or suggest the claimed invention.

### *Claim Amendments*

The foregoing amendment of claim 1 specifies a computer-implemented method of single sign-on user access to multiple web servers. Support for the foregoing amendment is found throughout the specification and in the claims. Accordingly, no new matter has been added.

### *Claim Rejections - 35 U.S.C. § 101*

Claims 1-19 stand rejected under 35 U.S.C. 101 because the Examiner now considers that the claimed invention is directed to non-statutory subject matter in that claim 1 uses the words “authenticating”, “detecting”, “transmitting”, “authenticating the authentication token”, and “providing”, which words the Examiner further considers to be “non-statutory subject matter because they consist on software process steps without any application to a hardware device.”

While specific authority for such proposition is not readily apparent, the premise is simply wrong in that claim 1 clearly recites, for example, “authenticating a user by a first web server”, “detecting a client request ... at said first web server”, “transmitting the encrypted authentication token from the first web server to the second web server via the user’s web browser”, “authenticating the authentication token by the second web server”, and “providing the second type of service session functionality ... by the second web server.”

Nevertheless, the foregoing amendment specifying a “computer-implemented method of single sign-on user access to multiple web servers” overcomes the Examiner’s rejection of independent claim 1 and claims 2-19 that depend on claim 1.

***Claim Rejections - 35 U.S.C. § 112***

Claims 1-19 stand rejected under 35 U.S.C. 112, first paragraph, because the Examiner considers that “the specification does not disclose, ‘a first type of service session...’, and a ‘second type of service session’” and the Examiner further considers “‘a first type of service session...’” and ‘a second type of service session’ as authenticating a user to create an encrypted authentication token and redirecting a web browser of the user to transmit the encrypted authentication token”.

Turning first to the Examiner’s statement that “the specification does not disclose, ‘a first type of service session...’, and a ‘second type of service session’”, as explained in the “Background” section of the application:

Such an entity or group of entities may wish to allow their customers access to such an aggregated functionality by signing on only once, by authenticating themselves once, and then being able to use different services which might be provided either by different servers of entities within the group of entities, or by servers of the group of entities and, for example, by servers of third party entities. Application, p. 1, lines 20-25.

As further explained in the example embodiment described with reference to Figs. 1-3:

Once the customer logs into the brokerage firm web site 32, the web site 32 presents the customer 10 with a welcome page from the web site 32. Once logged in, the customer 10 may examine the customer’s brokerage account information, portfolio, investment information, and the like. Application, p. 5, lines 14-17.

....

Referring again to FIG. 2, the customer 10 requests bill payment 50 by clicking on the “bill payment” hyperlink 102. The brokerage firm web server 30 itself does not handle the process of bill payment, but the server 30 is programmed with the knowledge that the bank web server 40 handles such a process. The hyperlink 102 includes the URL of the bank web site 42. Upon detecting the request of bill payment, the brokerage firm server 30 builds an authentication token 52. An authentication token comprises an object (or data) that can be passed between cooperating servers. A function of an embodiment of an authentication token is to convey the necessary information from a primary (or first) server to a secondary (or second) server to allow the secondary server to skip the sign-on process that would otherwise be necessary and required. Once a primary server establishes a session for a user, a cooperating secondary server that receives a valid authentication token from the primary server can establish a session without having the user sign on again. Application, p. 5, lines 24-p. 6, line 5.

....

The customer client 10 receives the web page 100 and proceeds with the bill-payment session with the bank server 40. In an embodiment, the authentication token (cookie) is then discarded or destroyed by the web server 40. Application, p. 12, lines 21-24.

Thus, the Examiner’s statement that the specification does not disclose first and second types of service session functionality, as recited in claim 1, is likewise simply wrong, in that the foregoing passages clearly describe an example embodiment in which a first type of session service functionality comprises a brokerage type of session service functionality at the brokerage firm web site 32 where the customer 10 may, for example, examine the customer’s brokerage account information, portfolio, investment information, and the like, and a second type of session service functionality that comprises a banking type of session service functionality at the bank web site 40 in which the customer can conduct a bill-payment session.

Turning next to the Examiner's statement that "a first type of service session" and "a second type of service session", as recited in claim 1, must both be construed as "authenticating a user to create an encrypted authentication token and redirecting a web browser of the user to transmit the encrypted authentication token", again the statement is simply wrong in that it completely disregards and is completely contrary to the plain language of the limitations of claim 1, such as "the first web server also providing a first type of service session functionality for the user in addition to an authentication functionality", "a second type of service session functionality for the user ... that is not provided by the first web server", and "a second web server providing the second type of session functionality for the user."

***Claim Rejections - 35 U.S.C. § 102***

Claims 1-19 and 25-43 stand rejected as anticipated by the Sasmazel (U.S. Patent No. 6,263,432) under 35 U.S.C. § 102(e). The rejection is traversed and reconsideration is requested.

The rejection of independent claims 1 and 25 is based primarily on the incorrect premise proposed by the Examiner that the first and second types of service session functionality provided at the first and second web servers, respectively, consist of authenticating the user, creating the authentication token, and redirecting the user's web browser to the second web server. It is readily apparent that the limitations recited in claim 1 of the first web server "providing a first type of service session functionality for the user in addition to an authentication functionality" and the second web server providing the "second type of service session functionality for the user ... that is not provided by the first web server" preclude the Examiner's claim that the service session functionality provided at both web servers consists of authenticating the user, creating the authentication token, and redirecting the user's web browser.

Sasmazel fails to teach or suggest one or more limitations recited in each of independent claims 1 and 25 in at least the following respects:

- Instead of a first web server that also provides a first type of service session functionality for the user in addition to an authentication functionality, as recited in claims 1 and 25, Sasmazel relies on a dedicated authentication server 350 which provides no type of service session functionality other than the authentication functionality. Thus, According to Sasmazel, when the user submits a sign-on request to the web server 220 or 240, instead of authenticating the user by a first web server that also provides a first type of service session functionality for the user in addition to the authentication functionality, as recited in claims 1 and 25, the web server 220 or 240 of Sasmazel sends the user's sign-on request to the dedicated authentication server 350, which then generates an "eticket" 310. See, e.g., Sasmazel, Col 7, line 38-Col 10, line 30 and Figs. 6 and 7.
- Instead of detecting a client request for a second type of service session functionality at the first web server that is not provided by the first web server, determining a second web server which provides the second type of session functionality, creating an encrypted digitally signed authentication token and redirecting the user's browser to the second web server by the first web server, and transmitting the token from the first web server to the second web server, as recited in claims 1 and 25, according to Sasmazel, after generating the "eticket" 310, the dedicated authentication server 350 simply sends the "eticket" back to the user's browser 210, where it remains until the user signs on again at the same or another web server 220 or 240 to request another function, at which time, the "eticket" is sent from the browser to the particular web server 220 or 240, which in turn sends the "eticket" on to a dedicated authorization server 360. See, e.g., Sasmazel, Col 10, lines 9-24 and Fig. 7.
- Instead of authenticating the authentication token and providing the second type of service session functionality for the user (i.e., that is not provided by

the first web server) by the second web server, as recited in amended claims 1 and 25, according to Sasmazel, when the user signs on again at the same or another web server 220 or 240 to request another function and the “eticket” is sent to the particular web server, the web server 220 or 240 sends the “eticket” to the dedicated authorization server 360, which performs the authentication and authorization check, and if validated by the authorization server, the validation is returned to the other web server 220 or 240. See, e.g., Sasmazel, Col 10, lines 20-30 and Fig. 7.

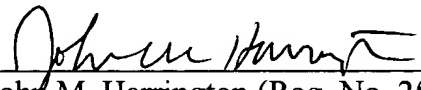
Consequently, Sasmazel fails to teach the required combinations of limitations of Applicants’ method and system of single sign-on user access to multiple web servers as recited in independent claims 1 and 25. Because each and every element as set forth in independent claims 1 and 25 is not found, either expressly or inherently in the cited reference, the Examiner has failed to establish the required *prima facie* case of unpatentability. See Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628 (Fed. Cir. 1987); See also MPEP §2131. The Examiner has failed to establish the required *prima facie* case of unpatentability for independent claims 1 and 25 and similarly has failed to establish a *prima facie* case of unpatentability for claims 2-19 that depend on claim 1 and claims 26-43 that depend on claim 25, and which recite further specific elements that have no reasonable correspondence with the references.

### Conclusion

In view of the foregoing amendment and these remarks, each of the claims remaining in the application is in condition for immediate allowance. Accordingly, the examiner is requested to reconsider and withdraw the rejection and to pass the application to issue. The examiner is respectfully invited to telephone the undersigned at (336) 607-7318 to discuss any questions relating to the application.

Respectfully submitted,

Date: 10/17/05

  
John M. Harrington (Reg. No. 25,592)  
for George T. Marcou (Reg. No. 33,014)

Kilpatrick Stockton LLP  
607 14th Street, NW, Suite 900  
Washington, DC 20005  
(202) 508-5800